

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
«ДОНЕЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ»**



Затверджено рішенням вченої ради ДонНТУ
Протокол від 21.05 2020 р. № 3
Голова вченої ради

[Signature] Я. О. Ляшок/

Освітня програма вводиться в дію з 2020_/21_ н.р.
наказом від 21.05 2020 р. № 253

**ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА
«Кібербезпека»**

Рівень вищої освіти	Перший	
Ступінь вищої освіти	Бакалавр	
Спеціальність	125	Кібербезпека
Галузь знань	12	Інформаційні технології
Кваліфікація	Фахівець із організації інформаційної безпеки	

Покровськ – 2020__ р.

ЛИСТ ПОГОДЖЕННЯ
освітньо-професійної програми

Освітня програма обговорена та схвалена на засіданні вченої ради факультету комп'ютерних наук і технологій

Протокол № 4 від 24.04. 2020р.

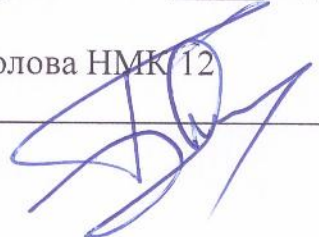
Голова вченої ради ФКНТ

 С.О. Ковальов

Освітня програма обговорена та схвалена на засіданні науково-методичної комісії ДонНТУ з галузі знань 12 Інформаційні технології.

Протокол № 4 від 28.04. 2020р.

Голова НМК 12

 Є.О. Башков

Начальник навчально-методичного відділу  /Г. С. Панченко/
« 28 » 04, 2020р.

ПЕРЕДМОВА

Освітньо-професійна програма (ОП) розроблена відповідно до Стандарту вищої освіти за спеціальністю 125 Кібербезпека для першого (бакалаврського) рівня вищої освіти, наказ МОН № 1074 від 04.10.2018 р.

Розроблено робочою проектною групою у складі:

<u>Прізвище, ім'я, по батькові</u>		<u>Посада та назва підрозділу</u> (в дужках - за основним місцем роботи)
Керівник робочої проектної групи (гарант освітньої програми):	1. Маслова Наталія Олександрівна	Доцент кафедри прикладної математики та інформатики
Члени робочої проектної групи:	2. Башков Євген Олександрович	Професор кафедри прикладної математики та інформатики
	3. Назарова Ірина Акопівна	Доцент кафедри прикладної математики та інформатики

Рецензії-відгуки зовнішніх стейкхолдерів (за наявності):

<u>Прізвище, ім'я, по батькові</u>	<u>Посада та назва організації (за основним місцем роботи)</u>

Освітня програма введена у 2020 р.

Термін перегляду освітньої програми: раз на 5 років.

<u>АКТУАЛІЗОВАНО:</u>			
Дата перегляду освітньої програми			
Підпис			
Прізвище, ім'я, по батькові гаранта освітньої програми			
Рішення Вченої ради ДВНЗ «Донецький національний технічний університет»			

Ця освітня програма не може бути повністю або частково відтворена, тиражована та розповсюджена без дозволу ДВНЗ ДонНТУ.

1. Профіль освітньої програми

1.1 – Загальні відомості	
<u>Повна назва вищого навчального закладу (відокремленого структурного підрозділу)</u>	Державний вищий навчальний заклад «Донецький національний технічний університет»
<u>Ступінь вищої освіти та назва кваліфікації мовою оригіналу</u>	Перший (бакалаврський) рівень Фахівець з організації інформаційної безпеки
<u>Офіційна назва освітньої програми</u>	Кібербезпека
<u>Тип диплому та обсяг освітньої програми</u>	Диплом бакалавра, одиничний, 240 кредитів ЄКТС, термін навчання 3 роки 10 місяців
<u>Наявність акредитації</u>	Сертифікат про акредитацію серія УД № 05008640, виданий 23.04.2019р. Термін дії сертифіката до 01 липня 2024 р.
<u>Цикл/рівень</u>	НРК України – 7 рівень, FQ-EHEA - перший цикл, EQF-LLL - 6 рівень
<u>Передумови</u>	Умови вступу визначаються «Правилами прийому до ДВНЗ «Донецький національний технічний університет», затвердженими Вченою радою університету. На базі атестата про повну загальну середню освіту
<u>Мова(и) викладання</u>	Українська
<u>Термін дії освітньої програми</u>	до 01.07.2024 р.
<u>Інтернет-адреса постійного розміщення опису освітньої програми</u>	http://wiki.donntu.edu.ua/view/Категорія:Освітні_програми
1.2 – Мета освітньої програми	
Підготовка висококваліфікованих фахівців в галузі інформаційних технологій зі спеціальності 125 Кібербезпека, здатних вирішувати типові та складні завдання та проблеми забезпечення захисту інформаційних ресурсів у кіберпросторі для подальшої професійної діяльності у галузі інформаційної та/або кібербезпеки.	
1.3 – Характеристика освітньої програми	
<u>Предметна область</u>	Галузь знань: 12 Інформаційні технології Спеціальність: 125 Кібербезпека
<u>Орієнтація освітньої програми</u>	Освітньо-професійна програма пропонує комплексний підхід до вирішення сучасних проблем управління кібербезпекою. Дисципліни та модулі програми засновані на теоретичних знаннях, які тісно пов'язані з практичними навичками. Студенти отримають необхідні навички та знання у забезпеченні захисту об'єктів інформатизації, включаючи комп'ютерні, автоматизовані, телекомунікаційні, інформаційні, інформаційно-аналітичні, інформаційно-телекомунікаційні системи, інформаційні ресурси й інформаційні технології.
<u>Основний фокус освітньої програми та спеціалізації</u>	Акцент у освітній програмі робиться на здобутті навичок та знань в галузі захисту інформаційних активів та ґрунтується на здатності випускників здійснювати професійну діяльність на підприємствах, діяльність яких пов'язана з процесами збору, обробки та розповсюдження інформації різного рівня з застосуванням інформаційних та комунікаційних технологій.
<u>Особливості програми</u>	Програма зорієнтована на підготовку фахівців, діяльність яких пов'язана з забезпеченням безпеки інформаційних та

	комунікаційних технологій. Високий рівень дослідницької частини підготовки забезпечується потужною науковою школою на чолі з доктором технічних наук, професором Башковим Є.О., розвиненою міжнародною співпрацею в науковій і освітній сфері
1.4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Фахівець може займати первинні посади (за ДК 003:2010): Відповідно до здобутого освітнього ступеню бакалавр здатний виконувати професійні роботи за професіями, зазначеними у ДК 003:2010 Національний класифікатор України. Класифікатор професій, а саме: 3439. Фахівець з організації інформаційної безпеки 3121. Фахівець з інформаційних технологій
Подальше навчання	Можливість продовження освіти за другим (освітньо-науковим) рівнем вищої освіти.
1.5 – Викладання та оцінювання	
<u>Викладання та навчання</u>	Студенто-центроване навчання, технологія проблемного і диференційованого навчання, технологія інтенсифікації та індивідуалізації навчання, технологія програмованого навчання, інформаційна технологія, технологія розвивального навчання, кредитно-трансферна система організації навчання, електронне навчання в системах дистанційної освіти (Moodle), самонавчання, навчання на основі досліджень. Викладання проводиться у вигляді: лекції, мультимедійної лекції, інтерактивної лекції, семінарів, практичних занять, лабораторних робіт, самостійного навчання на основі підручників та конспектів, консультації з викладачами, підготовка кваліфікаційної роботи бакалавра.
<u>Оцінювання</u>	Оцінювання навчальних досягнень здійснюється за 100-бальною (рейтинговою) шкалою, національною 4-х бальною шкалою («відмінно», «добре», «задовільно», «незадовільно») і вербальною («зараховано», «незараховано») системами. Види контролю: поточний, тематичний, періодичний, підсумковий, самоконтроль. Форми контролю: усне та письмове опитування, тестові завдання в тому числі комп'ютерне тестування, лабораторні звіти, презентації, захист курсових робіт та проектів, звітів з практик, захист кваліфікаційної роботи бакалавра.
1.6 – Програмні компетентності	
Інтегральна компетентність	Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі кібербезпеки або у процесі навчання, що передбачає застосування теорій та методів інформаційних технологій і характеризується комплексністю та невизначеністю умов.

Загальні компетентності (ЗК)	<p>ЗК01. Здатність застосовувати знання у практичних ситуаціях.</p> <p>ЗК02. Знання та розуміння предметної області та розуміння професії.</p> <p>ЗК03. Здатність спілкуватися рідною та іноземною мовами як усно, так і письмово</p> <p>ЗК04. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням</p> <p>ЗК05. Здатність до пошуку, оброблення та аналізу інформації.</p> <p>ЗК06. Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні;</p> <p>ЗК07. Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.</p>
Фахові компетентності спеціальності (ФК)	<p>ФК01. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та Міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки</p> <p>ФК02. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки</p> <p>ФК03. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах</p> <p>ФК04. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.</p> <p>ФК05. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.</p> <p>ФК06. Здатність відновлювати штатне. Функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.</p> <p>ФК07. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.)</p> <p>ФК08. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.</p> <p>ФК09. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою.</p> <p>ФК10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності.</p> <p>ФК11. Здатність виконувати моніторинг процесів</p>

	функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки. ФК12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.
1.7 - Програмні результати навчання	
ПРН01.	Застосувати концептуальні знання з навчальних дисциплін загальної підготовки для засвоєння навчальних дисциплін професійної підготовки;
ПРН02.	Організувати власну професійну діяльність, обирати та способи розв'язування складних спеціалізованих задач та практичних проблему професійній діяльності, оцінювати їхню ефективність;
ПРН03.	Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності;
ПРН04.	Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення;
ПРН05.	Адаптуватися в умовах часткої зміни технологій професійної діяльності, прогнозувати кінцевий результат;
ПРН06.	Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності
ПРН07.	Діяти на основі законодавчої, нормативно-правової баз України та вимог відповідних стандартів, тому числі міжнародних в галузі інформаційної та/або кібербезпеки;
ПРН08.	Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та/або кібербезпеки;
ПРН0	
9.	Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки;
ПРН10.	Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем;
ПРН11.	Виконувати аналіз зав'язків Між інформаційними процесами на віддалених обчислювальних системах;
ПРН12.	Розробляти моделі загроз та порушника;
ПРН13.	Аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандарт. технологіях та протоколах передачі даних;
ПРН14.	Вирішувати завдання захисту програм та інформації, що обробляється В інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень;
ПРН15.	Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій;
ПРН16.	Реалізовувати комплексні системи захисту інформації В автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів;
ПРН17.	Забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент;
ПРН18.	Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів;

ПРН19. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах;
ПРН20. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах;
ПРН21. Вирішувати задачі забезпечення та супроводу (в .т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки В інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах;
ПРН22. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і/або кібербезпеки;
ПРН23. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів В інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах;
ПРН24. Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових);
ПРН25. Забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту;
ПРН26. Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем;
ПРН27. Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах;
ПРН28. Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та/або кібербезпеки;
ПРН29. Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів;
ПРН30. Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем;
ПРН31. Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем;
ПРН32. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки;
ПРН33. Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків;
ПРН34. Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації;
ПРН35. Вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і/або кібербезпеки;
ПРН36. Виявляти небезпечні сигнали технічних засобів;
ПРН37. Вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність

захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації;	
ПРН38. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації;	
ПРН39. Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах;	
ПРН40. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації;	
ПРН41. Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур;	
ПРН42. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки;	
ПРН43. Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/або кібербезпеки для розслідування інцидентів;	
ПРН44. Вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами;	
ПРН45. Застосовувати різні класи політик інформаційної безпеки та/або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів;	
ПРН46. Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах;	
ПРН47. Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації;	
ПРН48. Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах;	
ПРН49. Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах;	
ПРН50. Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних);	
ПРН51. Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах;	
ПРН52. Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах;	
ПРН53. Вирішувати задачі аналізу програмного коду на наявність можливих загроз.	
ПРН54. Усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.	
1.8 — Ресурсне забезпечення реалізації програми	
Кадрове забезпечення	Викладання професійно-орієнтованих дисциплін здійснюють науково-педагогічні працівники, які мають наукові ступені та вчені звання. До викладання будуть залучені також фахівці, у яких є науковий ступінь та працюють в галузі інформаційних технологій.

Матеріально-технічне забезпечення	Забезпеченість навчальними приміщеннями, комп'ютерними робочими місцями, мультимедійним обладнанням відповідає потребі. Користування Інтернет-мережею безлімітне. Для проведення досліджень наявна комп'ютерна техніка.
Інформаційне та навчально-методичне забезпечення	Підручники, навчальні посібники та періодичні наукові видання з інформаційних технологій, захисту інформації та кібербезпеки. Підручники та навчальні посібники до викладання дисциплін циклу професійної підготовки, які розміщені у фонді наукових бібліотек ДВНЗ «ДонНТУ» м. Покровськ, а також Національній бібліотеці України ім. В.І. Вернадського, Інтернет ресурсах та авторських розробках науково-педагогічних працівників ДВНЗ «ДонНТУ». Офіційний веб-сайт https://donntu.edu.ua . містить інформацію про освітні програми, навчальну, наукову і виховну діяльність, структурні підрозділи, правила прийому, контакти. Матеріали навчально-методичного забезпечення освітньо-наукової програми викладені на освітньому порталі: http://donntu.edu.ua .
1.9 - Академічна мобільність	
Національна кредитна мобільність	Індивідуальна академічна мобільність реалізується у рамках між університетських договорів про встановлення науково-освітніх відносин для задоволення потреб розвитку освіти і науки з ВНЗ України. Можливість здійснювати підготовку фахівців за індивідуальними програмами, що відповідають потребам конкретного виробництва, згідно з умовами відповідних договорів між університетом і підприємствами.
Міжнародна кредитна мобільність	Не здійснюється
Навчання іноземних здобувачів вищої освіти	Не здійснюється

2. ПЕРЕЛІК КОМПОНЕНТ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ ТА ЇХ ЛОГІЧНА ПОСЛІДОВНІСТЬ

2.1. Перелік компонент ОП

<u>Код компонента</u>	<u>Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики і атестації)</u>	<u>Кількість кредитів</u>	<u>Форма підсумкового контролю</u>
Обов'язкові компоненти			
<i>Цикл загальної підготовки</i>			
OK1	Іноземна мова. Частина 1	4,0	іспит
OK2	Вища математика. Частина 1	7,0	іспит/ІНД
OK3	Ділова українська мова	4,0	іспит
OK4	Фізичне виховання (загальна підготовка). Частина 1	3,0	диф. залік
OK5	Фізика	7,0	іспит
OK6	Іноземна мова. Частина 2	4,0	іспит
OK7	Вища математика. Частина 2	7,0	іспит/ІНД
OK8	Історія України та української культури	5,0	іспит
OK9	Фізичне виховання (загальна підготовка). Частина 2	3,0	диф. залік
OK10	Філософія	4,0	іспит
OK11	Теорія ймовірностей та математична статистика	6,0	іспит
OK12	Правознавство	5,0	іспит
OK13	Безпека життєдіяльності та охорона праці	4,0	іспит
Всього по циклу:		63	
<i>Цикл професійної підготовки</i>			
OK14	Основи алгоритмізації	5,0	іспит/ІНД
OK15	Програмування	6,0	іспит/ІНД
OK16	Дискретна математика	5,0	іспит
OK17	Основи інформаційної безпеки	5,0	іспит/КП
OK18	Об'єктно-орієнтоване програмування	5,0	іспит/ІНД
OK19	Чисельні методи	6,0	іспит/ІНД
OK20	Організація баз даних	5,0	іспит/КП
OK21	Системне програмування	5,0	іспит
OK22	Безпека та захист операційних систем	6,0	іспит
OK23	Теорія сигналів та процесів	6,0	іспит/ІНД
OK24	Математичні методи криптографії	6,0	іспит/ІНД
OK25	Криптографічні протоколи	6,0	іспит/КП
OK26	Інформаційно-телекомунікаційні системи	5,0	іспит/ІНД
OK27	Архітектура систем захисту інформації (КСЗІ)	5,0	іспит
OK28	Безпека програм та даних	5,0	іспит/ІНД
OK29	Захист розподілених баз даних та інформаційних систем	6,0	іспит
OK30	Управління інформаційною безпекою	5,0	іспит
Всього по циклу:		92	
<i>Практики і атестації</i>			
OK31	Навчальна практика	4	диф. залік
OK32	Виробнича практика	4	диф. залік
OK33	Переддипломна практика	3	диф. залік
OK34	Випускна кваліфікаційна робота	12	атестація
Всього по циклу:		23	
Загальний обсяг обов'язкових компонент:		178	

Вибіркові компоненти			
Вибір за блоками (професійна підготовка)			
Вибірковий блок 1			
ВБ 1.1	Комбінаторні методи захисту інформації	5,0	іспит/ІНД
ВБ 1.2	Основи безпеки в Інтернет	5,0	іспит
ВБ 1.3	Захист комп'ютерних мереж	6,0	іспит
ВБ 1.4	Методи приховування інформації	5,0	іспит
ВБ 1.5	Методи аналізу даних	5,0	іспит/ІНД
ВБ 1.6	Технології створення криптографічних додатків	5,0	іспит
Вибірковий блок 2			
ВБ 2.1	Додаткові розділи комбінаторного аналізу	5,0	іспит/ІНД
ВБ 2.2	Безпека Web-додатків	5,0	іспит
ВБ 2.3	Протоколи передачі даних	6,0	іспит
ВБ 2.4	Основи стеганографічних перетворень	5,0	іспит
ВБ 2.5	Емпіричні методи кібербезпеки	5,0	іспит/ІНД
ВБ 2.6	Інформаційна безпеки спеціалізованих систем	5,0	іспит
Всього по циклу:		31	
Вибір з переліків			
ВБ3 ДВС 2	Вибіркова дисципліна з переліку 1 Вибіркова дисципліна з переліку 2 Вибіркова дисципліна з переліку 3 Вибіркова дисципліна з переліку 4	5,0	диф. залік
ВБ4 ДВС 3	Вибіркова дисципліна з переліку 1 Вибіркова дисципліна з переліку 2 Вибіркова дисципліна з переліку 3 Вибіркова дисципліна з переліку 4	5,0	іспит
ВБ5 ДВС 4	Вибіркова дисципліна з переліку 1 Вибіркова дисципліна з переліку 2 Вибіркова дисципліна з переліку 3 Вибіркова дисципліна з переліку 4	6,0	іспит
ВБ6 ДВС 5	Вибіркова дисципліна з переліку 1 Вибіркова дисципліна з переліку 2 Вибіркова дисципліна з переліку 3 Вибіркова дисципліна з переліку 4	5,0	іспит
ВБ7 ДВС 6	Вибіркова дисципліна з переліку 1 Вибіркова дисципліна з переліку 2 Вибіркова дисципліна з переліку 3 Вибіркова дисципліна з переліку 4	5,0	іспит
ВБ8 ДВС 7	Вибіркова дисципліна з переліку 1 Вибіркова дисципліна з переліку 2 Вибіркова дисципліна з переліку 3 Вибіркова дисципліна з переліку 4	5,0	іспит
Всього по циклу:		31	
Загальний обсяг вибірових компонент:		62	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		240	

2.2. Структурно-логічна схема ОП

Структура освітньої програми «Кібербезпека» спеціальності 125 Кібербезпека. Рік вступу 2020

1 семестр		2 семестр		3 семестр		4 семестр		5 семестр		6 семестр		7 семестр		8 семестр	
Освітні компоненти	К	Освітні компоненти	К	Освітні компоненти	К	Освітні компоненти	К	Освітні компоненти	К	Освітні компоненти	К	Освітні компоненти	К	Освітні компоненти	К
Іноземна мова. Частина 1	4	Іноземна мова. Частина 2	4	Філософія	4	Чисельні методи ІНД	6	Безпека та захист операційних систем	6	Криптографічні протоколи КП	6	Правознавство	5	Управління інформаційною безпекою	5
Вища математика. Частина 1	7	Вища математика. Частина 2	7	Теорія ймовірності та математична статистика ІНД	6	Організація баз даних КП	5	Теорія сигналів та процесів ІНД	6	Інформаційно-телекомунікаційні системи ІНД	5	Безпека життєдіяльності	4	Технології створення криптографічних додатків	5
												Безпека програм та даних ІНД	5	Інформаційна безпека спеціалізованих систем	
Ділова українська мова	4	Історія України та української культури	5	Основи інформаційної безпеки КР	5	Системне програмування	5	Математичні методи криптографії ІНД	6	Архітектура систем захисту інформації (КСЗІ)	5	Захист розподілених баз даних та інформаційних систем	6	ДВС7	5
Фізичне виховання. Частина 1	3 залік	Фізичне виховання. Частина 2	3 залік	Об'єкто-орієнтоване програмування ІНД	5	Основи безпеки в Інтернет	5	Захист комп'ютерних мереж	6	Методи приховування інформації	5	Методи аналізу даних ІНД	5		
						Безпека Web-додатків		Протоколи передачі даних		Основи стеганографічних перетворень		Емпіричні методи кібербезпеки ІНД			
Фізика	7	Програмування ІНД	6	Комбінаторні методи захисту інформації ІНД	5	ДВС3	5	ДВС4	6	ДВС5	5	ДВС6	6		
Основи алгоритмізації ІНД	5	Дискретна математика	5	Додаткові розділи комбінаторного аналізу ІНД											
				ДВС2	5 дз	Навчальна практика	4			Виробнича практика	4			Переддипломна практика	3
														Випускна кваліфікаційна робота	12
	30		30		30		30		30		30		30		30

Освітні компоненти	
	Обов'язкові дисципліни загальної підготовки
	Обов'язкові дисципліни професійної підготовки
	Практики
	Атестації
	Дисципліни вільного вибору студента

3. ФОРМА АТЕСТАЦІЇ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

Атестація випускників освітньої програми проводиться у формі захисту випускної кваліфікаційної роботи та завершується видачою документів встановленого зразка про присудження йому ступеня бакалавр зі спеціальності 125 Кібербезпека та присвоєнням професійної кваліфікації «Фахівець із організації інформаційної безпеки».

Атестація здійснюється відкрито та публічно.

4. МАТРИЦЯ ВІДПОВІДНОСТІ ПРОГРАМНИХ КОМПЕТЕНТНОСТЕЙ КОМПОНЕНТАМ ОСВІТНЬОЇ ПРОГРАМИ

[illegible]

Позначки програмних компетент- ностей та освітніх компонентів	ВБ 1.1	ВБ 1.2	ВБ 1.3	ВБ 1.4	ВБ 1.5	ВБ 1.6	ВБ 2.1	ВБ 2.2	ВБ 2.3	ВБ 2.4	ВБ 2.5	ВБ 2.6	ВБ3 ДВС2	ВБ4 ДВС3	ВБ5 ДВС4	ВБ6 ДВС5	ВБ7 ДВС6	ВБ8 ДВС7
ЗК01						+						+						
ЗК02	+						+											
ЗК03		+		+				+		+								
ЗК04			+						+									
ЗК05					+						+							
ЗК06		+						+										
ЗК07				+						+								
ФК01		+																
ФК02							+											
ФК03						+												
ФК04			+															
ФК05												+						
ФК06									+									
ФК07			+															
ФК08	+																	
ФК09						+												
ФК10		+																
ФК11											+							
ФК12					+													

Примітки:

1. ОКі - певний обов'язковий компонент освітньої програми за розділом 2.1;
2. ВБі - певний вибірковий блок освітньої програми за розділом 2.1;
3. ЗКі - загальна компетентність за розділом 1.6 профілю освітньої програми;
4. ФКі - фахова компетентність за розділом 1.6 профілю освітньої програми;
5. • - позначка, яка означає, що певна програмна компетентність забезпечується певним освітнім компонентом поточного рядка.

5. МАТРИЦЯ ЗАБЕЗПЕЧЕННЯ ПРОГРАМНИХ РЕЗУЛЬТАТІВ НАВЧАННЯ (ПРН) ВІДПОВІДНИМИ КОМПОНЕНТАМИ ОСВІТНЬОЇ ПРОГРАМИ

[illegible]

ПРН25												+						
ПРН26												+						
ПРН27		+	+					+	+									
ПРН28	+				+		+					+						
ПРН29					+													
ПРН30												+						
ПРН31				+							+							
ПРН32		+						+				+						
ПРН33												+						
ПРН34												+						
ПРН35												+						
ПРН36			+						+									
ПРН37			+						+									
ПРН38			+		+				+		+							
ПРН39												+						
ПРН40												+						
ПРН41				+						+		+						
ПРН42												+						
ПРН43												+						
ПРН44	+						+											
ПРН45												+						
ПРН46												+						
ПРН47	+			+			+			+								
ПРН48												+						
ПРН49					+						+							
ПРН50												+						
ПРН51					+						+							
ПРН52												+						
ПРН53						+												
ПРН54							+											

Примітки:

1. ПРНі - певний результат навчання за розділом 1.7 профілю освітньої програми;
2. * - позначка, яка означає, що певний програмний результат забезпечується освітнім компонентом поточного рядка.

Завідувач кафедри
прикладної математики
і інформатики



О.А. Дмитрієва

Керівник робочої (проектної) групи
(гарант освітньої програми)



Н.О. Маслова